(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 May 2001 (10.05.2001)

PCT

(10) International Publication Number
WO 01/33359 A1

(51) International Patent Classification[7]: G06F 11/30, H04L 9/00

(21) International Application Number: PCT/US00/30420

(22) International Filing Date:
3 November 2000 (03.11.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/163,477 3 November 1999 (03.11.1999) US

(71) Applicant: ANDERSEN CONSULTING L.L.P. [US/US]; 100 South Wacker Drive, Chicago, IL 60603 (US).

(72) Inventors: LUM, Robert; 5727 N. East Circle Ave., Chicago, IL 60631 (US). SWAHN, Martin; Apt. 22, Villa Azzurra, 5, boulevard du Cap, F-06600 Antibes (FR). JONES, Ruth, P.; W251S4386 Oak View Drive, Waukesha, WI 53189 (US).

(74) Agent: OKEY, David, W.; Brinks Hofer Gilson & Lione, P.O. Box 10087, Chicago, IL 60610 (US).

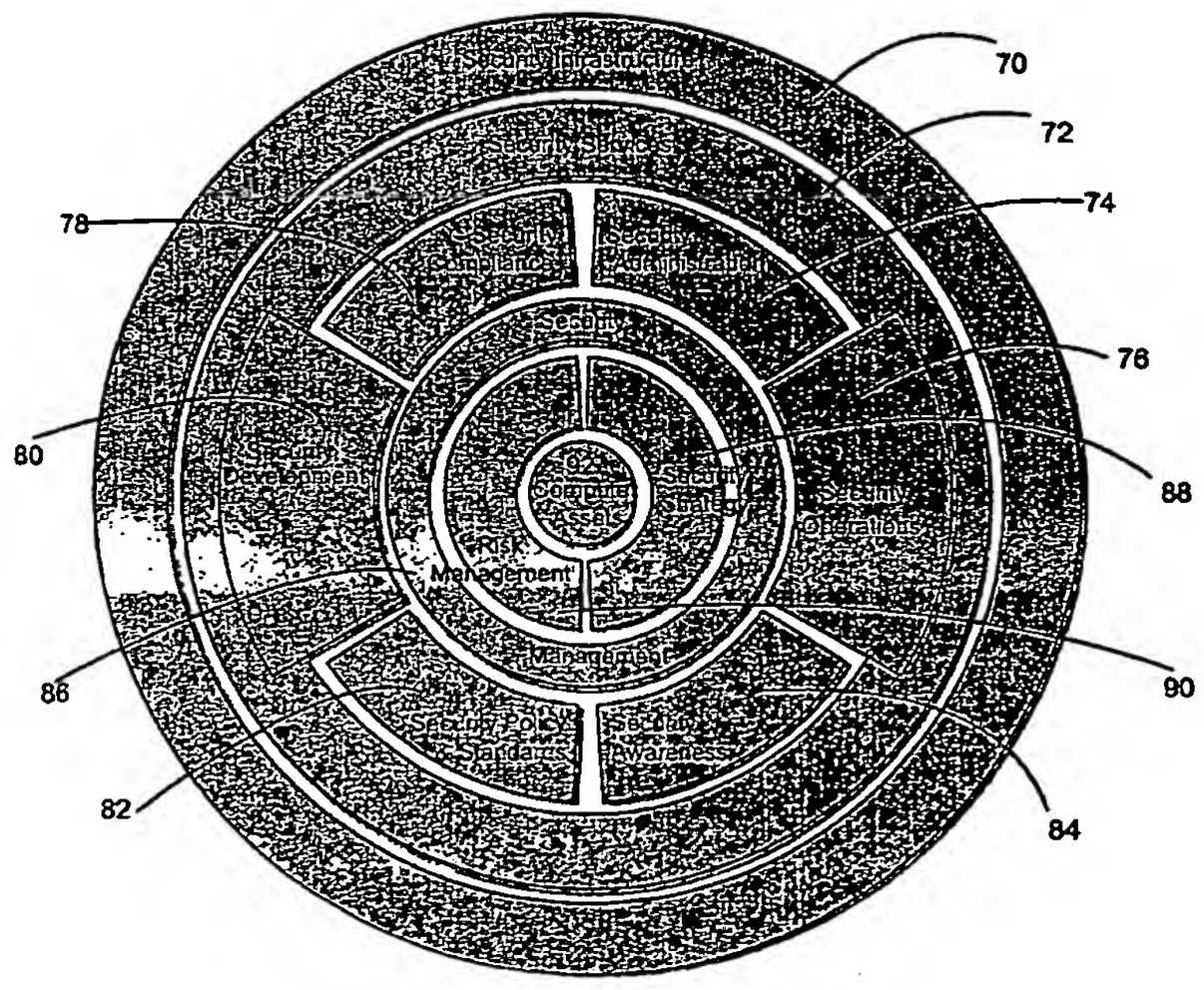
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

[Continued on next page]

(54) Title: NETCENTRIC COMPUTER SECURITY FRAMEWORK



(57) Abstract: A security framework (70) useful for providing security for users in a computer system. The framework (70) comprises a security infrastructure and security services (72). The key to providing a secure computer system is to provide the basic security components (70-90), tools, services and to implement them with security policy (82) and standards (82) awareness.

WO 01/33359 A1

— *Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

NETCENTRIC COMPUTER SECURITY FRAMEWORK

RELATED APPLICATIONS

The present application claims the benefit of U.S. Provisional Application No. 60/163,477, filed November 3, 1999, which is incorporated by reference herein.

BACKGROUND OF THE INVENTION

The importance of information as an asset to a business or an enterprise is increasing. More and more information is computer-based and accessible in all areas of daily life, including sensitive and confidential information on assets, commerce, spending, credit, education, finance, government, and health. The rapid growth of e-Commerce as an effective way to conduct business is just one more example of the importance and use of information in daily life. As a result, computer security has become more important than ever before. Computer viruses encumber and disable networks and systems worldwide, while hackers penetrate computer systems, causing havoc and committing fraud. The increasing need for security becomes clear when considering security as an enabler of many of the trends in the marketplace. Examples of these trends are a shift towards more distributed and Internet-base computing environments, such as e-Commerce and large corporate networks.

In many ways, computer security can be viewed as a business capability in itself. It is very important to use sophisticated security solutions in order to avoid fraud, protect assets, and protect clients and customers from unauthorized access or transactions. A computer security system should

unauthorized access or transactions. A computer security system should assure confidentiality of information, as well as information integrity—assurance that the information is accurate, authentic and complete. The information must also be available, with information systems functioning, when the information is desired.

What is needed is a computer security system that will allow speedy access, but will still protect the vital information assets of an organization, whether the organization is a business, a non-profit or educational organization, a charity, a governmental body, or other useful enterprise. What is needed is a computer security system that will protect information, but still allow ease of electronic transactions among computers, and applications residing on corporate networks, and the Internet.

BRIEF SUMMARY OF THE INVENTION

One aspect of the invention is a security architecture for a netcentric computer system, comprising a network, a server for the network, and a client connected through the network with the server, and a computer security system protecting the network, the server and the client. The server may be one or more, of several types, including but not limited to, network, application and data servers. The security system includes both the technical architecture and core capabilities to protect computer assets. The technical architecture of the security system includes a security infrastructure and security services. The core capabilities of the security systems include the functions that are provided by the technology, the organization or enterprise, and their processes. Computer assets include the network, servers, clients, and the applications and data provided on these systems. Of course, the server may in actuality serve a plurality of clients, and the security system may be called upon to interact and protect them all.

Another aspect of the invention is a method of providing a netcentric security framework in a computing system. The method includes providing a security infrastructure for the system and providing security services for the system. The method also includes developing and maintaining security

procedures, processes, policies and standards for the system. The method includes conducting secure operations within the computing system, and making users aware of the need for computer security. It is recognized that it is prudent, as well as easier, to design a computer system with security built-in, rather than adding the security framework after a computer system has been designed and built. Therefore, while the security framework described herein may be used as an add-on, it is preferable to design a security architecture into the first stages of a computer system.

These and other features and advantages of the invention will become apparent upon review of the following detailed description of the presently preferred embodiments of the invention, taken in conjunction with the appended drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention is illustrated by way of example and is not limited to the accompanying figures. In the figures, like reference numbers indicate identical or functionally similar elements.

Fig. 1 is a diagram of a relatively simple architecture suitable for business-to-consumer e-commerce.

Fig. 2 is a diagram of a more complex and robust architecture, suitable for business-to-business e-commerce.

Fig. 3 is a diagram of a more complex network suitable for use in an enterprise with remote offices, remote customers and remote users.

Fig. 4 is a schematic diagram of a security architecture framework.

Fig. 5 is a flow chart for design and operation of a security framework.

DETAILED DESCRIPTION OF THE INVENTION

Information assets, including that are addressable by computer, should be protected. These assets include all forms of information and the people and technology that support the information processes. Information assets addressable by or for computers are computer assets. Computer assets may include such things as private data, technology environment data, application

data, application services, people services, and technology services. Information may be in many different forms, computer addressable and otherwise, including, but not limited to, computer data files, tapes, discs, videos, packets, paper, conversation, or any medium that conveys knowledge or ideas. Information not addressable by computer may be transformed by one of many methods, including a microphone, scanning, data entry, and so on. The information then becomes both a computer asset and an information asset. Information processes include creation, management, storage and transport.

Private data may include, but is not limited to, personnel data, financial data, account data, e-mails, knowledge capital, contractual data, business or enterprise data or proposals or plans, and so on. Technology environment data may include, but is not limited to, user IDs and passwords, security configurations, network configurations, system software, custom software, vendor software, encryption keylists, and the like. Application data includes, but is not limited to, development software, test data, client software, client configuration data, and the like. Application services include, but are not limited to, accounts payable, order processing, manufacturing management, inventory management, materials management, and the like. People services include, but are not limited to, hardware installation, software installation, configuration management, code development, change control, backups, monitoring, and the like. Technology services include, but are not limited to, network connectivity, logon, access control, and so on.

One aspect of the invention is a security architecture for a computer system. The architecture comprises information assets and processes to be protected, core security capabilities or functions, called core security components, and a technology architecture that comprises a plurality of tools and services that cooperate to provide security for the users and operators of a computer, a computer network, or an Internet site. A security infrastructure consists of the actual security components, tools and services which provide protection for the business assets. Security services such as an authentication service or encryption service are implemented using the

security components in the security architecture. The core security components provide an implementation method or technology for the security services. For example, authentication services may be implemented using either certificates or tokens.

In addition to the technical features, a variety of non-technical features are also required to implement a workable security framework. These non-technical features are a product of the management of the system, and include inputs from a variety of functions or organizations within an enterprise. A first basic step is to identify the assets to be protected. Are all computer assets, whether data, or programs or applications, identified properly and placed in a secure environment? The security strategy of a business or an enterprise may answer the question of just how secure the business assets need be, with respect to the inherent inconvenience of technical security features. The risk management function or organization of the enterprise may also have an input into the security strategy.

Other non-technical aspects of a security system or infrastructure may include security management of the enterprise or the computer system. How loose or how tight security policy and standards are set will determine how secure the computer operation, databases, and information remain. Are users required to change passwords at regular time intervals? Also important in protecting assets is the general tone of security compliance and security awareness among users. Are unguarded terminals available to casual users? Do terminals or personal computers "remember" passwords so that any user may log on and access data?

While the security components and services are highly important technical aspects of computer security, it is also important that an enterprise seeking to protect assets should have a policy for ongoing security development. As times and technologies change, the enterprise's need for security will also change. Security operations must ultimately be monitored by people and by management, or there will be very little security. A business or an enterprise should be vigilant in its security compliance and administration, and its security operations should be important both to users

and to management. This is inherently difficult in a netcentric computer environment, where an enterprise will often connect its systems to those of its customers, partners, service providers, and perhaps even its competitors.

Designing the complex security architecture required to satisfy the needs of today's distributed, mission-critical applications is a major challenge. As such, it is helpful to have an inventory of components that may be required for the design, build, installation and operation of systems. It is also helpful to have an understanding of how the components fit together conceptually. In one embodiment of the invention, the core security components include, but are not limited to, registration and identification, authentication, single sign-on, access control, encryption, digital notarization, content and virus inspection, logging, non-repudiation, firewall, public key infrastructure (PKI), platform security, and virtual private networks (VPN).

REGISTRATION AND IDENTIFICATION

Registration and identification refers to the process of creating new users in a system. Ensuring proper identification and registration of users is necessary to allow effective authentication. With the evolution of the Netcentric environment, on-line registration has become a popular method for obtaining access to specific resources via the Internet. It allows customers to register and modify information about themselves that is stored by the host site. Included as part of registration and identification are data verification services, registration authority, and directories or meta-directories. Secure socket layers may be used for encryption of the data entered during the registration process.

Data verification services verify data such as address, social security number or other data submitted during registration for the purpose of ensuring the integrity of the data. This can be done through financial institutions or government services. This is critical if a strong authentication service is to be implemented.

Registration Authorities are used in Public Key Infrastructures (PKI). The role of the Registration Authority is to certify that a public key is

associated with a known entity (the entity may be an individual or a system). After authenticating the identity of the entity, a certificate is generated and assigned to the entity. The robustness of the identification and authentication step determines the strength of the certificate. The security requirements of the business capability will determine the strength of the certificate needed.

Registration information is often stored in an enterprise-wide directory or meta-directories server. Advantages of directories are performance, compared to a traditional database, and their usefulness as a central repository for user profiles. An example would include customer information or certificates. Directory standards include X.500 and the Lightweight Directory Access Protocol (LDAP). LDAP directories are typically used for storing and retrieving certificates and certificate revocation lists. A directory may be used as a meta-directory providing mapping between UserIDs in different systems. This is useful when data in older legacy systems cannot be changed.

AUTHENTICATION

Authentication is an enabler for many other security functions, for example access control, and is often the first security measure an end-user will see. Authentication, when implemented in a complete security architecture, will be transparent to the end-user and yet secure enough to control access to a network. Authentication is the process of identifying and ensuring that an entity is who it claims to be. For individuals this is usually based on a username and password. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual. The architecture may include many forms of authentication. These forms or methods include, but are not limited to, user name and password, token and one-time password, certificates, time-dependent passwords, and biometrics. Computer components that implement these methods of authentication include an authentication server, directories, and PKI. These forms and methods are defined below.

Username/Password is one-factor authentication in its simplest and most common form. Username/Password authentication can be implemented using many standards and technologies. Advantages are ease of use, low cost and portability. Pure username/password authentication provides only basic authentication. A security architecture with username/password must implement encryption when transferring the username/password. Authentication standards include: RADIUS, TACACS, TACACS+, RACF, NT login and UNIX login. The major weakness of password-based authentication is the ease of breaking it with password-guessing and brute-force techniques. It is important to educate users about strong password policies, and to enforce the policies with password monitoring processes.

Token and one time password is a two-factor authentication which uses a hardware device that generates a one time password to authenticate its owner. It is also sometimes applied to software programs that generate one-time passwords. This authentication is also known as a challenge response mechanism. SecurID and Enigma Logic are examples of password calculator products

Certificates are part of PKI. Certificates may be implemented for individual users or for systems such as individual servers. Different classes of certificates can be generated with defined levels of trust. The highest levels of trust are typically used in financial transactions and where confidentiality requirements are high. Different types of certificates are required for specific cryptographic protocols such as secure socket layers (SSL), secure multi-purpose Internet Mail Extensions (S/MIME) or Internet Protocol Security (IPSEC). The X.509 standards define the data in a certificate. Other standards include Public Key Crypto Systems (PKCS), PKCS#6, PKCS#9, and PKCS#10. Certificates are commonly stored in a directory.

A time dependent password is a password that is valid only at a certain time of day or during a specified interval of time. Depending on how the passwords are made available to the users (a printed list of passwords changed daily, a token card, etc.), this authentication approach can be considered as either one-factor or two-factor. Biometrics is the science and

technology of measuring and statistically analyzing biological data. This is sometimes considered a three-factor authentication by adding the concept of "what you are" (i.e. fingerprint) to "what you know" (i.e. password) and "what you have" (i.e. token card). In information technology, biometrics usually refers to technologies for measuring and analyzing human body characteristics such as fingerprints, eye retinas and irises, voice patterns, facial patterns, and hand measurements, especially for authenticating an individual user.

Smartcards are credit card-sized devices that can be used to store information. They typically contain an integrated circuit with secure memory and hardware support for security functions. The chip can store data and a variety of application programs that can be updated whenever necessary. A high level of security protects the card issuer as well as the cardholder from unauthorized access. Typical applications are bankcards, travel cards, and campus cards. Smartcards can be used for electronic purses, personal identification, building access, and payments. A PIN code is necessary to activate the smartcard. Smartcards are considered two-factor authentication.

An authentication server is a central server which authenticates and authorizes access to requested systems or services. The purpose of an authentication server is to centralize and standardize the interface to and from multiple authentication services. The authentication server will maintain user profiles in a central database that all remote servers can share. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point. Having a central service also means that it is easier to track usage for billing and for keeping network statistics. One of the most common ways to implement this is via RADIUS. RADIUS is a client/server protocol and software that enables remote access servers to communicate with a central authentication server to authenticate dial-in users and authorize their access. RADIUS is a de facto industry standard. Radius is commonly used with a directory server over LDAP.

Directories support multiple authentication methods, such as Username/ Password and digital certificates. Applications query the directory

by passing it appropriate security data (for example a Username/Password) and receiving back either a message indicating the success or failure of the request. Advantages of directories are fast performance and their ability to function as a central repository for user profiles (for example customer information, certificates, etc.). Directory standards include X.500 and LDAP. LDAP directories are typically used for storing and retrieving certificates and certificate revocation lists (CRL). Public Key Infrastructure(PKI) is a networked system of certificate authorities (CAs), registration authorities (RAs), certificate management systems (CMSs) and X.500 or LDAP directories. It enables two parties unknown to each other to exchange sensitive information over an unsecured network like the Internet. PKI uses public and private keys to authenticate and encrypt information.

SINGLE SIGN-ON

Single sign-on enables a user to sign on using a single UserID and be connected to multiple systems without having to sign on to each one of them. Single sign-on provides two main benefits: a user-friendly system and a system that is easy to administer. Sub-components and systems of single sign-on include cookies and session management, access control products, scripting solutions, and password synchronization.

Cookies / Session Management – in order to provide single sign-on capabilities, session management functions are needed. Session management is a service which keeps track of each open session between entities, such as between servers and clients. Session management is usually implemented with a token that is passed between the client and server. The token is sometimes called a cookie. The token may also be posted within a URL. The token contains a session ID and other information required to maintain a separate identity for each session. For additional security, the token often contains timestamps and the IP address of the client to prevent spoofing or hijacking a session. Session management techniques are commonly used on the Internet to provide personalization, such as "shopping cart" features on a consumer retail site.

Single sign-on across multiple servers is more complex. It involves transferring the session information among distributed servers. A distributed session management architecture can implement such functions, and commercial products for this purpose are becoming more common. Session management with cookies and URL-based tokens uses the functionality built into HTML browsers. To prevent eavesdropping or replay attacks, the information carried in the token should be encrypted.

An access control product provides single sign-on through the use of advanced session management as described in Cookies / Session Management, and additionally provides for authentication, authorization and access control. Advanced access control products can provide single sign-on capabilities across numerous servers. Scripting solutions are single sign-on solutions which provide strong authentication of the user as part of the initial sign-on. Once this has been accomplished, sign-on to all the other applications and resources take place through their individual sign-on protocols, but they are automated and transparent to the user.

Scripting solutions and products work through a scripting language that is used to develop login scripts for each application or system. The scripts issue the commands and transfer information needed by each application or system for user authentication and access to resources. The login information required for the remote applications and systems must be encrypted and stored securely. Similarly, the transmission of login information to the remote applications and systems must also be secure.

Password synchronization allows users to authenticate to different services using the same password. Password synchronization may be an element of an "Enterprise User Management" solution. Password synchronization operates by having participating systems monitor user password changes. When a user changes his/her password, the monitor communicates the new password to other systems. This is known as "propagation" of the password change. Often, the password synchronization system will enforce password quality requirements (e.g., length, composition,

history, etc.). Examples of systems using password synchronization are NIS and NIS+, NDS, and Windows NT domains.

Single sign-on can provide many benefits and a quick return on investment if implemented well. In a Netcentric environment a single sign-on solution may be a way to gain access to many new and older systems. The security requirements need to be high, as a single point of access into multiple systems in a network is dangerous, should it be compromised. One important aspect is to ensure that the operations environment can provide high availability and good performance. A single sign-on solution may become a single point of failure.

ACCESS CONTROL

Access control refers to the process of limiting access to the resources of an IT system to only authorized users, programs, processes, systems or other IT products. There are several access control methods that may be implemented in many places in an information technology, or computer, environment. These methods include, but are not limited to, firewalls, operating systems, network operating systems, access control products, Web access control, and role-based access control.

A firewall provides for access control by restricting packet types, protocols, filters, sockets, ports, services and providing network address translation (NAT). Firewalls can also provide authentication, encryption and access control based on users and groups. Firewalls can be implemented as hardware or software. A firewall is an essential part of Netcentric security architectures. Firewalls are commonly implemented for network perimeter security. For access control firewalls are highly effective as they limit unwanted communication to an internal network. Firewalls are usually combined with other access control mechanisms such as access control products, web access control or operating system access control.

Operating Systems and network operating systems also provide for access control. Operating systems such as Unix and Windows NT provide for control by multiple access parameters. Examples include user, group, time of

day, workstation address, files and directories. Network Operating System access control is similar to Operating System access control, and access parameters may include user, group, time of day, workstation address, files and directories.

Specific access control products provide advanced access control. In addition to Operating System access control, more control of access to resources can be provided. This is done by using additional conditions that are checked to verify whether access should be granted. An example would be to grant access if the user a) belongs to the finance group, b) logs in between 7am and 7pm, and c) has been employed more than 6 months. The access control products may be interfaced with corporate databases, by using structured query language (SQL) for example, to enable conditional access control.

Web Access Control tools are specifically designed for use in Netcentric environments together with web/application servers. They are able to provide a high granularity of access control. They provide access control and resource protection by installing a plug-in component for the web/application server which intercepts all incoming HTTP requests. By examining the HTTP request, it is possible to determine the resource being accessed. The web access control product can protect all resources which are accessible via a URL from a browser. Examples of these resources include, but are not limited to, HTML pages, cgi-scripts, Java applications, business applications, databases, objects on an HTML page, links, etc. Web access control products also provide authentication, authorization, single sign-on and logging services.

Role-based access control is based on assigning access rights for resources to a role, not to an individual. An individual is then assigned a role and inherits the access rights of the role. While holding that role the individual can perform all actions for which the role has authorization. The benefit of role based access control is that it is easier to administer. For example: if an employee quits, his or her roles can be removed and assigned to a replacement. This alleviates the problem of deleting user accounts and

creating new ones every time an employee changes jobs. An individual may have several roles. Example roles are: preferred customer, administrator, executive team, finance director, etc. A complete role based system requires significant work to determine which roles are necessary and which functions they should be authorized to perform. Careful design is therefore required. Usually a matrix of all roles and the functions performed is used during the design process.

ENCRYPTION

Encryption is the process of making information unreadable to protect it from unauthorized viewing or use, especially during transmission or storage. Encryption is based on a cryptographic algorithm and at least one key. Even if the algorithm is known, the information cannot be decrypted without the key(s). There are several methods to implement encryption, including public key cryptography, symmetric keys, one-time pads, key-stream generation, and hardware-based cryptography.

Public Key Cryptography is a type of cryptography that uses a key pair of mathematically related cryptographic keys. The public key can be made available to anyone who wishes to use it and can encrypt information or verify a digital signature; the private key is kept secret by its holder and can decrypt information or generate a digital signature. Because of the relatively large keys and slow speed, its use is generally limited to the encryption of small amounts of data, such as distribution of symmetric keys, authentication, and digital signature creation and verification. Public Key Cryptography relies on a Public Key Infrastructure (PKI). A public key infrastructure (PKI) is a set of security services that enable the use of public-key cryptography and certificates in a distributed computing system. Within security domains, PKI enables the use and management of both encryption keys and certificates, providing services such as key management (including key updates, recovery and escrow), certificate management (including generation and revocation), and policy management.

A secret key or symmetric key is shared between the two entities in a transaction. The success of secret key encryption depends upon the encryption keys being kept secure from all others besides the communicants. For such encryption to be usable and useful, support must be provided for the generation of unique keys, their storage, distribution, retirement, replacement, and secure retrieval. In particular, secure symmetric key management mandates a strong policy of hardware-enforced key separation. This is a high priority requirement for financial institutions doing financial transactions around the world. The most common implementation of a symmetric key is the Digital Encryption Standard (DES). A key-exchange protocol is a protocol interaction or mechanism for symmetric key encryption to exchange the secret key between two unrelated entities in a transaction.

A one-time pad is a very simple yet completely unbreakable and secure symmetric cipher. It relies on a completely random key which must be kept safe. One-time pads are used by intelligence agencies around the world and where the confidentiality requirements are extremely high. Key-stream generation algorithms are encryption algorithms which change keys during transmission. These rely on two key stream generators which must remain synchronized for the process to work successfully.

For increased security and performance a hardware based encryption device may be considered. Hardware encryption provides secure key storage and recovery mechanisms. Hardware encryption offloads the computationally intensive public key operations from the server to a cryptographic hardware module, thus eliminating the bottlenecks associated with software cryptographic functions. Functionality provided by hardware encryption includes a cryptographic co-processor for key generation, certificate generation, certificate and signature verification, signing, and hashing.

DIGITAL NOTARIZATION

Digital Notarization is the process of ensuring that electronic information, such as a document or file, contained specific content at a specific moment in time and can be proven to not have been modified since

then. Digital notarization consists of three tools, including digital signature, hashing, and time-stamping of computer-generated files. PKI may also be used to provide Digital Notarization.

Digital Signature is a cryptographic method provided by public key cryptography and used by a message's recipient and any third party to verify the identity of the message's sender. It can also be used to verify the authenticity of the message. A sender creates a digital signature or a message by transforming the message into a message digest and encrypting it with his or her private key. A recipient, using the sender's public key, verifies the digital signature by applying a corresponding transformation to the message and the signature. PKI may be used to create digital signatures that prove that a unique individual has created a document.

Time stamping is a method used by corporations and professionals to notarize, time-stamp and validate any type of computer-generated file, including e-commerce transactions, email correspondence, database records, word processing documents, images, and video clips. Companies can use it to detect any type of tampering with electronic data. Time stamping prevents adding, deleting data or backdating transactions. Time stamping provides tamperproof security, especially critical in industries such as financial services, e-commerce, and industries in which intellectual property and regulatory data must be protected.

Time stamping uses a hashing algorithm to create a unique document fingerprint, also known as a message digest. It is effectively impossible to change any of the documents without changing the hash values. When a document's authenticity needs to be verified, the hash value for the document is mathematically calculated from the published root hash. If the calculated hash value matches the document's hash value it can be concluded that the document has not been altered.

Hashing is an algorithm used to create a message digest of a document. Hashing algorithms take a message of any length and, using a one-way function, compute a unique message digest of a constant length. Since a one-way function is used, the message cannot be recreated from the

result. This process will always yield the same result from identical starting data, but it is extremely unlikely that two different messages could produce the same result. The message digest can then be encrypted using the originator's private key and sent with the message. The recipient can compute the message digest of the received message using the identical hash function, decrypt the message digest sent with the message using the originator's public key, and compare the results. If a single bit of information has been changed during transmission, the two digests will differ, and the recipient will know that the integrity of the message is suspect and should be discarded. Standards include: SHA, MAA, MAC, MD2, MD4 and MD5.

CONTENT/VIRUS INSPECTION

There is always a chance that content arriving contains harmful data or applications. Content / Virus Inspections provide a method to detect and remove any harmful content before it can cause damages. Tools available include mobile code inspection, e-mail filtering, and anti-virus software.

Mobile Code Inspection is a method to protect an internal network from receiving hostile content. Mobile code inspection occurs at the gateway, away from critical resources, and can identify potential hostile attacks before they enter the network. Mobile code inspection allows control, management and enforcement of corporate-wide security policy for Java, ActiveX, JavaScript, Visual Basic Script, Plug-ins, URLs, Cookies and other content. Mobile code inspection works with leading firewall products. Mobile code inspection is commonly also implemented at the client as well as server level.

Similar to mobile code inspection, e-mail filtering takes place at the gateway. E-mail filtering can protect the a computer environment from e-mail threats before they reach their network and compromise business or enterprise assets. Corporate-wide or enterprise-wide security policies may be implemented with e-mail filtering technologies to monitor e-mail usage.

Anti-virus software is a requirement for any network connected to the Internet. Anti-virus technologies will scan incoming traffic and e-mails for viruses. Anti-virus technologies can also scan e-mail attachment for hostile

applications. Anti-virus software is commonly implemented at the server level and client level. Some firewalls provide anti-virus functionality. A point solution for anti-virus should be taken into consideration because general purpose anti-virus solutions may not provide protection as strong as a point solution. Any anti-virus solution needs to be updated regularly.

LOGGING

Logs are the primary method to trace problems and security breaches in a network or IT system. By logging events from multiple devices an operator can trace the events leading up to a problem and determine the cause of the problem. Logs can be used in prevention as well as in reaction to a threat. There are two methods to implement logging, centralized and distributed.

Centralized Event Logging is used to record the occurrence of significant events. An event may be, for example, a user logon, an addition to a file, or a change to a user's privileges. Centralized event logs provide a centralized collection point for security events, error reports, system alerts, diagnostic messages, and status messages generated by a system. Event logs are especially important for system security to help track and trace the actions of users in a system. Centralized event logging is commonly implemented by using simple network management protocol (SNMP) event management. SNMP events can be interfaced to an enterprise operations management system to record and log all security events centrally. The benefit of using a centralized system is that all the information can be correlated and analyzed more easily. These security events come from many devices, for example, intrusion detection tools, custom applications, operating systems, network routers, web/application servers, etc.

In distributed logging, each device and application writes to its own log file. The solution is not connected to an enterprise operations management system. A log scanning tool may be used to collect the most important events and create reports. These tools can be configured to run at specific intervals. Security events for all devices should be recorded. When designing the

logging architecture it is important to take performance and network traffic into consideration. Examples of what events and activities to log are found in Table 1.

NON-REPUDIATION

Non-repudiation is a method used to prove that certain actions have taken place and cannot be denied. A Digital Signature is a reliable cryptographic method of signing electronic documents that provides sender authentication, message integrity and non-repudiation. Digital signatures provide a convenient, time-saving, and secure way of signing electronic documents. Digital signatures provide stronger evidence of the authenticity of information than a hand-written signature, which could easily be forged. A digital signature is provided by public key cryptography. It may be used by a message's recipient and any third party to verify the identity of the sender and non-repudiation of origin. Digital signatures can also be used to verify the authenticity of the message as a digital notarization service. Standards include DSA and DSS.

TABLE 1 SECURITY LOG AND ACTIVITIES

Type of Log	Information contained in the log
User activity	Login activity User ID changes File accesses by the user Authorization information Authentication information
System Activity	System restarts and shutdowns Administrative shutdowns
Network Connections	Details (when, where, what kind) of connections attempted or established Details of connections established
Network Traffic Monitoring	Records of all network traffic transactions
Web Server Activity	Remote hostname or IP address Date and time of request

Request response code indicating whether request was successful
Remoter login name of user (if available)
Username used for authentication (if available)

FIREWALL

A firewall is a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria. Three types of firewalls use techniques of packet filtering, application proxy, and stateful inspection. Firewalls are also used to set up secure communications via an encrypted channel, a so-called Virtual Private Network (VPN).

Packet filtering firewalls provide access control at the network layer. They accept, reject or drop packets of data based on the source/ destination computer network address and the type of application being accessed. For example, FTP and Telnet are commonly restricted. Packet filtering firewalls can also restrict traffic by time of day, day of week, etc. Packet filtering firewalls are highly effective for implementing a company's network security policy. A packet filtering firewall can be implemented using hardware such as a network router. There are also many purpose-built firewalls which perform packet filtering.

An application proxy firewall serves as a proxy for the internal server. The proxy establishes a connection to the internal server on behalf of the external user, copies the data received from the server and then retransmits it to the user. This method ensures that an intruder will not use the actual server containing the data and other sensitive information. The application proxy is commonly placed in the demilitarized zone (DMZ). Access to the

application proxy is possible only from the IP address of the external packet filtering firewall, on specified protocols/ports, and from the IP address of the internal packet filtering firewall.

Stateful packet inspection uses communication- and application-derived state and context information to regulate packet traffic. The state and context information is stored and updated dynamically. This method can allow, for example, an FTP upload connection, but disallow packets with commands that switch directories during the session. Stateful inspection is a powerful tool allowing high granularity of the access control.

PUBLIC KEY INFRASTRUCTURE (PKI)

PKI consists of several components, including certificate management, certificate authority, key management, and time-stamping. The tools used to implement PKI are PKI toolkit and third party management. Certificate Management includes certificate repository, certificate revocation and cross-certification. A Certificate Authority is an entity authorized to issue certificates. Key Management provides key updates, key backup/recovery, key history, and key encryption algorithm. Keys can be created as private/public key pairs or as a private key only (shared secret). Time Stamping may be used to prevent adding, modifying, deleting data or backdating transactions. Time stamping provides tamperproof security. These components are used to verify and authenticate the validity of each party involved in an Internet transaction. PKIs are currently evolving and becoming more widespread.

The methods to implement PKI include PKI toolkits, which allow a company to build and integrate a PKI. Administration and management of the PKI is performed internally. This service is intended for organizations that demand the data security and access control enabled by digital certificates and choose to build and operate their own system. There is considerable overhead to maintain a PKI and manage the life-cycle of a digital certificate. One benefit is increased control. A drawback is that rigorous security and

facilities must be implemented to protect the infrastructure. An example of a PKI Toolkit vendor is Entrust.

Third party management is a service is intended for organizations that demand the data security and access control enabled by digital certificates, but choose not to build and operate their own system. Instead, they rely on the infrastructure and management of the PKI by third party companies. The benefit is that the third party vendor will manage the infrastructure and have the secure facilities to do so. The drawback is a loss of control and a requirement for trust in the vendor. An example of a vendor providing PKI services is Verisign.

PLATFORM SECURITY

It is important to secure the platform on which sensitive servers and applications run. A failure to secure the platform, and all interconnecting lines (WAN, LAN, Ethernet, etc.) may result in the platform, server and application being compromised. There are many publicized articles about the vulnerabilities in servers and applications. Many of them are a result of weaknesses in the underlying platform. Platform security may be provided by hardened operating systems, or by active security enforcement. Essential to platform security is policy enforcement.

A hardened operating system (OS), also known as a bastion host, provides for confidential, secure network communications within a defined trusted networking environment. A hardened OS includes specific security enhancements compared to standard OS versions. It can also be used to provide a hardened base for applications needing a higher level of trust, such as a Web server or application server. A hardened OS is essentially a bare-boned operating system, specifically designed for high security environments. Many of the normal OS services, such as FTP and Telnet, have been taken out and only core services required for specific functionality are enabled. A hardened OS is resistant to buffer overflows and other vulnerabilities found in a normal OS. By using protected memory space, a 'sandbox' is created for each service or application to limit the harm they can do.

Active security enforcement tools proactively control access to data and applications located on servers throughout an organization. There are two approaches to active security enforcement, application programming interfaces (APIs) and event management.

By integrating security application through an API, interoperability between security products is provided. Two major initiatives are under way Adaptive Network Security Alliance (ANSA) and Open Platform for Secure Enterprise Connectivity (OPSEC). API integration will provide powerful integration between security tools. The downside is that they are time consuming to implement and it may take some effort to maintain compatibility with all products supplied by different vendors. Two competing standards are emerging, ANSA driven by Internet Security Systems (ISS) and OPSEC driven by Check Point.

Event Management, on the other hand, uses industry standard event management and can be integrated into already existing enterprise operations management systems. The active security enforcement components communicate with each other via SNMP events to a central console that filters, correlates and takes action on security events. This form of active security enforcement is essentially an advanced form of event management specifically for security. Upon detection of a hostile security event a policy may be executed which shuts down a compromised server. This solution is driven by Network Associates.

Policy enforcement is a tool used to perform scheduled and selective probes of network operating systems to search for those vulnerabilities most often used by unscrupulous individuals to probe, investigate, and attack networks. This tool can be used to eliminate identified vulnerabilities.

Platform security is an important measure to secure an environment. A hardened OS is a requirement, for example, in financial transactions. Active security enforcement is an important security management tool which can be integrated with a wider enterprise operations management framework. Policy enforcement should be used on all servers exposed on a network. It will eliminate the most common ways of penetrating a network or server.

VIRTUAL PRIVATE NETWORK (VPN)

A VPN, also known as an encrypted tunnel, is built atop a public network, such as the Internet. Hosts within the VPN use encryption to talk to other hosts. The encryption excludes hosts from outside the VPN even if they are on the public network. For two hosts to communicate with each other, a VPN must be established between the two hosts. The two key standards for creating a VPN tunnel are IP Security (IPSec) and Layer 2 Tunneling Protocol (L2TP). Together L2TP and IPSec provide complementary approaches to solid, secure tunneling.

At the initiation of a VPN, public keys are used to authenticate the users and exchange symmetric keys. The symmetric keys are then used as the session key for encrypting subsequent traffic. Symmetric keys provide faster performance than public/private keys. Depending on the level of trust in a network and security requirements, VPN are implemented in two ways, personal tunnels and groups.

Where a network is not trusted a VPN is established end-to-end between the hosts. This means that the connection starts, for example, at a workstation and ends at the server with which it communicates. This provides higher security, but also adds to a more complex implementation because each client wishing to establish a VPN needs client software. Group tunnels are commonly implemented on firewalls. The VPN starts at the firewall and ends at a firewall. This assumes that the network is trusted from the firewall to the desktop, which is not part of the encrypted tunnel. The advantage is that no client software is required. All encryption is performed by the servers or firewalls.

When implementing a VPN consider the type of applications and network protocols which need to be encrypted and tunneled. This will determine which standard for use in creating and managing the tunnel. L2TP has the advantage of being able to encapsulate and tunnel other networking protocols such as IPX and SNA. IPSec works with the IP protocol. The two tunneling techniques can be used together.

The figures depict applications in which security components work and interact in order to provide security for a computer system, and in particular for a net-centric computer system. Fig. 1 depicts a computer system with a remote client 10 connected via the Internet 20 to Web Server 46 and an Application Server 50. The Application Server administers and cooperates with a mainframe computer 48 and a database 52, on which may reside data or functions useful for the server and the clients. The computer system on the server portion is protected first by a firewall 42 which may include a packet filter 30 as described above. An encryption server 44 may also be used for any of the encryption modes and methods mentioned.

Not shown in this figure but also useful, are any other of the security components. The computer system, for example, may require users to register and identify themselves for a first entry, followed by authentication for subsequent use of the server-mainframe-database system. The firewall, besides a packet filter, may also include authentication, access control, and encryption. In addition, the server computer system, whether on the mainframe or on a server, may also provide for single sign-on (perhaps not needed in the simple system shown in Fig. 1), content and virus inspection, logging, and in a commercial setting, non-repudiation.

Fig. 2 is a more complex netcentric computer system 40, in which there may be more than one merchant or "fulfillment system" 64, possibly including their own databases 62, whose security is not shown. A remote client 10 accesses merchants through the Internet 20. In one embodiment, banking services or payment services 22 are part of the network. The netcentric computer system 40, connected by an electronic commerce LAN, is protected by a number of security features, including a firewall 42 and its packet filter 30. In this embodiment, a netcentric system includes a web server 46, an application server 50, a database server 54 and an application database 52. In more complex systems there may also be a development server 56 for developing future web-products or services, and a staging server 58. For convenience, the system has one or more administration workstations 60. The security components mentioned above

may be useful in such a system, where some components reside primarily in the firewall, and others may reside in one or more servers cooperating with the security system to render the netcentric system secure.

Fig. 3 depicts a corporate-type application for security frameworks and systems. Remote users, whether clients 10 or customers 12 access the netcentric system 40 through the Internet 20. The system may reside at corporate headquarters 13 or other convenient location, connected through a corporate Intranet 24 to other offices, such as local offices 14. The netcentric system 40 may be protected by a firewall 42 and other security components and systems. In one embodiment, the headquarters may use a workstation 17 to administer or manage the system, also allowing access to other internal users 18. The system may include any convenient number of computers or servers, such as a Web server 46, an application server 50, a database server 54 and a file transfer protocol server 55. All of these servers will require protection and security. The corporate local offices 14 may include client stations 16 as well as their own web servers 46 and application servers 50, and will thus require protection and security. In an industrial, or Business-to-Business setting, the customers 12 may also be corporate entities, with their own computer systems and their own need for computer security.

Fig. 4 depicts a technology architecture 70, 72 supported by security core capabilities 74, 76, 78, 80, 82, 84 that surround and protect business assets and key processes 86, 88, 90, 92 that require protection and security. The security system includes a technology architecture which includes a security infrastructure 70 and security services 72. The infrastructure and services are the technical measures taken to protect the assets.

The security framework includes core capabilities to a security system, including security administration 74 and security operations 76. Security compliance 78 is a desirable capability, as are any efforts toward security development 80. Other non-technical features, such as security policy and standards 82 and security awareness 84, may be important in maintaining a

secure system. A security policy is a set of rules, directives, and practices that regulate how an organization manages, protects and distributes sensitive information. A security policy is translated into access control rules that are enforced by the system.

The technology architecture and core capabilities protect computer assets and key processes. These include security management 86, which may include both technical and non-technical features. The overall security strategy 88 and risk management 90 of the enterprise play a part in designing and maintaining the security framework. Computer assets 92 may include, but are not limited to, computer assets of a business, an enterprise, or an organization. These assets may include, but are not limited to, a computer system, a network, a server, a client and an application and data provided on a computer system of the business, the enterprise, or the organization.

Fig. 5 is a flow chart for a method or process of designing and operating a security framework for a computer system, such as a netcentric computer system. A first step may include performing a risk assessment 91. Next, a designer of a computer system or its security framework should define a security policy 92, defined above, and translate that policy into access rules and determine the controls 93 for the security framework and the computer system. Once agreed upon, the control should be deployed or implemented 94 and managed 95 for compliance. Occasions may arise for a review of the controls 96, such as perceived or actual threats to computer security. System administrators or managers should respond appropriately to computer security events 97, and if necessary, repeat the process.

A first step in such a process is to perform a risk assessment 91, in light of any relevant security events. A risk assessment determines what is important, what needs protecting, and how much protection is desired. Risk assessments may include, but are not limited to, personal error that will inadvertently alter, release or lose information. Risk also includes natural disasters, such as fire or water damage that may destroy information. Risk includes misuse of data by legitimate users and malicious use of sensitive information. Risks may also include unauthorized access to files, systems or

networks. In addition, there may be risks to uncontrolled access to private data or uncontrolled modification of data (to which a user may have legitimate access). The security system is designed to provide controls to mitigate risks for the netcentric computer system.

Other steps in the process of Fig. 5 include defining the security policy, that is, to determine the functional requirements and to organize the policy by security services to meet the requirements. The security controls are then determined and a system designed to meet those needs. The design identifies the mechanisms and technologies that meet the system requirements. Part of implementing the security policy and controls may include a step of building, testing and evaluating the selected solutions, and verifying that the solution selected reduces the risks identified.

Security controls are managed by defining the organizational needs and procedures necessary to ensure that the solution maintains security during and after implementation. Security administration during this step may include loading users and profiles. Security administration also includes managing the users and ensuring proper security configurations and operations. Once the system is operating, controls may be reviewed to verify compliance and identify new exposures. Finally, the system should determine valid responses to security reviews, any threats, and new technologies that may apply.

SECURITY TOOLS

Security Tools support security management services and the people performing the security functions and processes. The tools help manage and control the security environment. The primary tools available are intrusion detection and vulnerability assessment.

Intrusion Detection tools, operating on a network of a platform, can detect suspicious activities on a network or on a platform. They work by recognizing common patterns that may indicate an attack. Intrusion detection tools provide a fast and automated mechanism that allows a company to be more pro-active in identifying and stopping intruders. Network tools act like a

network packet capture program, analyzing packets of information as they travel across the network, and interpreting hostile activity on the network by recognizing the network traffic patterns that indicate attacks. Platform tools detect intruders or abuse by analyzing audit data from the operating systems it supports. Using a rules engine, the tool spots obvious violations, such as multiple login failures. It also detects more subtle irregularities in user behavior that can indicate a masquerading user or other potential troublemaker.

Vulnerability assessment tools assist in finding common security holes and help to eliminate them by hardening them. Vulnerability assessments are generally performed on all hosts and servers, critical or non-critical. Often these tools measure against a set of criteria or standards. Vulnerability assessment tools assist in closing the gap between the security policy and actual security by providing information about security vulnerabilities. These tools typically probe operations on the network or the operating system.

Network probes perform scheduled and selective probes of network communication services, operating systems, and routers in search of those vulnerabilities most often used to probe, investigate, and attack the network. Network scans should include probing for auto-answer modems connected to the network. Operating system tools scan the operating system looking for common vulnerabilities. Vulnerabilities may include FTP and Telnet services, default user accounts, old and vulnerable versions of sendmail, patches not applied, xhost + enabled, etc. In addition, policy enforcement tools perform scheduled and selective probes of network operating systems to identify any discrepancies to the Security Policy of the company or enterprise.

Vulnerability assessment tools are very important to identify vulnerabilities so they can be eliminated. It is important to update vulnerability tools regularly. Users should plan for the processes that are needed to periodically run assessment tools, analyze the results, and respond to problems that are identified. Vulnerability assessment tools help meet the requirements of the Security Compliance area.

SECURITY SERVICES

Security services are re-useable common security architecture components which have been documented and packaged to facilitate easy re-deployment. In one embodiment, security services include both security base services and security management services. The objective of security services is to achieve consistency and standardization across the enterprise for common security functions such as authentication, encryption, etc. There are many advantages to the implementation of Security Services:

Consistency and standards in architecture.

Central administration and operations.

Shared development resources and less 're-invention'.

Reduced cost.

Increased speed of deployment and reduced time to market.

Higher security due to fewer solutions and systems for similar requirements.

Security Services are designed, built and implemented by a Security Development function as a result of requirements derived from the Security Strategy and Security Policy and Standards functions. A security architecture for a new business capability may be created by combining several existing Security Services and Security Infrastructure components.

SECURITY BASE SERVICES

Security Base Services are reusable components available to application developers to incorporate security functions into applications or business capabilities. A Security Base Service is implemented using one or more of the Core Security Components of the Security Infrastructure. There may be several implementation options for each Security Base Service. The security base services include, but are not limited to, registration and identification services, authentication services, single sign-on services, access control services, encryption services, digital notarization services, content and virus inspection services, logging services, and non-repudiation services.

ACCESS CONTROL SERVICES

Access Control refers to mechanisms and policies that restrict access to computer resources. Access control services are implemented to protect information Business Assets. Access control products often provide authentication and authorization services as well. There are multiple methods and locations to implement access control in a security architecture. The access control technology to use will depend on the general access control requirements and on the level of granularity that must be achieved. These may range from relatively basic user-based access control to complex, dynamic, role-based access control of individual data units.

A re-useable access control service will allow application developers to define the resources which should be protected and to then rely on the access control service to enforce security based on a set of access rules. It is important to determine where the access control should be located and what type of access control is required. Access control may be implemented at the firewall, web server, application server, database, network, etc., or a combination of these.

AUTHENTICATION

Authentication is the process of ensuring that an entity in a system transaction (including users, servers, and clients) is who he, she, or it claims to be. Authentication services are a means of enabling Access Control. Authentication is often divided into the following categories:

Knowledge-based – something a user knows (such as a password)

Token-based – something a user has (such as a smartcard)

Attribute-based – something a user is (biometric factors such as fingerprints)

Authentication can rely on a single technique ("one-factor" authentication), or on multiple methods used together ("two-factor" or "strong" authentication). Authentication services are used by applications and business capabilities in conjunction with Access Control services to protect resources. Two common ways to use authentication are to gain access to

systems and data, and to ensure that they are communicating with the intended entity. There are many different ways to implement authentication services and they provide various levels of authentication.

Username/Password based authentication is considered to be basic and widely implemented, but is the weakest method when used alone. If strong authentication is needed then two-factor authentication, for example token-based authentication that also requires a password, may be required.

SINGLE SIGN-ON

Single Sign-on services provide application developers a reusable and common interface by establishing a single UserID that can be used for access to multiple applications or systems. A single sign-on service in conjunction with an authentication service will eliminate the need for users to authenticate themselves to each application or system. A good single sign-on and authentication service architecture can pass the UserID to each application or system, which can then provide access to required resources on an individual basis. This is especially important in a Netcentric/Internet architecture.

A single sign-on service has many benefits. By taking advantage of a common UserID, the speed of application development is increased and time to market is reduced. Centralized control makes user administration easier since there is a single tool to create users, change passwords and delete users. Elimination of multiple authentication steps increases usability.

The security of a single sign-on service must be carefully designed. If properly designed and implemented, the security of the system will be higher. On the other hand, a poorly designed single sign-on service may add vulnerabilities to the system, since a security breach in the system may open up many other systems. In a diverse corporation or enterprise, a multiplicity of systems and applications poses a significant barrier to enterprise-wide single sign-on. Careful planning is required for each system that is to be included in the single sign-on capability. The use of pilots and incremental implementation of the single-sign-on capability may be necessary.

REGISTRATION/IDENTIFICATION SERVICES

The ability to effectively control access to system resources depends fundamentally on accurate identification of individuals during the registration process. Failure to do so properly may result in users gaining unauthorized access to system resources by impersonating a legitimate user. Ensuring proper identification and registration of users is especially important in a Netcentric environment, where users may register over the Internet.

Security requirements for registration and identification services should include simplicity and user friendliness, confidentiality and integrity for the submitted information, assigning roles to the registered user, ease of integration with host/legacy systems and business applications, and an ability to support many to many relationships. That is, the service should provide means to link new registration information to existing user data, and to map multiple UserIDs to a unique individual.

It is important to verify the identification data before registration. It is also important to consider factors such as future requirements, integration with host systems, usability, etc., when designing the Registration / Identification service.

ENCRYPTION

Encryption services protect information during transmission or storage with cryptographic techniques. Encryption services protect the privacy of a transaction, assure contents of the transaction cannot be altered without detection, and provide non-repudiation with digital signatures. Encryption services may be implemented either as hardware or software and in different layers, including, but not limited to, an application layer, a transport layer, a channel layer and a protocol layer. Application developers commonly implement encryption services using an encryption toolkit.

The specific implementation methods used for encryption are critical. Even if the cryptography algorithm employed is strong, a poorly designed implementation may introduce vulnerabilities that make it easy to break. There are several things to consider when implementing encryption, including

but not limited to, the management of encryption keys, the user interface design, encryption strength, performance implications, and legal implications.

DIGITAL NOTARIZATION

Digital Notarization services provide the ability to assign a timestamp and a digital signature to an electronic document: being able to prove that a document had a given content at a precise point in time and has not been altered. Digital Notarization services are becoming more important as the value of information and electronic transactions in e-Commerce grows.

CONTENT/VIRUS INSPECTION SERVICES

Content / Virus inspection services provide the means of inspecting, filtering and deleting harmful content before it causes damage to information systems. The Netcentric evolution has produced new technologies enabling new business opportunities. But with these new technologies, new threats in the form of viruses, hostile applets and other forms of downloadable executables, and e-mails have increased dramatically. This has put an even greater emphasis on the importance of proper security to protect against content threats.

Content / Virus inspection services are provided by firewalls and point solutions. Firewalls offer some protection in this area. In general, they are not focused on content / virus inspections, but more towards access control, authentication and encryption. Depending on the requirements, a firewall may be sufficient. Point solutions are tools specifically designed for protection against malicious mobile code, e-mail or viruses. The distinction between solutions for mobile code inspection, e-mail filtering and anti-virus is vague as many products provide some or all of the functionality found in the other categories.

An important factor to consider when implementing a Content / Virus Inspection service is that it must be updated regularly. Failure to update regularly will result in vulnerabilities to the system from new viruses and damaging forms of mobile code that are designed to circumvent existing

security measures. Proper Security Policy and Standards for monitoring new content threats and responding to them must be in place and must be enforced. Content / Virus inspection can be implemented either at the server or client level. Commonly both server and client protection is implemented as they complement each other. For laptop users it is a requirement to have client level protection in addition to what may be implemented at the server level.

LOGGING

Logging services provide a centralized repository for security-related events. A good security architecture uses the logging service to record all security events. This will provide Security Operations with the means of detecting security breaches and tracing them if an intruder penetrates the system. The logging service will ensure that the proper system information is recorded in a tamper-proof manner, since the logs may be used as evidence against an intruder.

Application developers may integrate application-specific security events with the logging service to benefit from the security monitoring functions provided by the Security Operations. Security Operations will need to cooperate with application developers to define which events to log. When designing a logging service, the following issues should be considered:

ADMINISTRATION

Security and integrity of the logs
The location of the data and files
Volume of data recorded
Performance implications
Log management and archiving
Who will analyze log information
How will the logs be analyzed?

NON-REPUDIATION

Non-repudiation services provide tamperproof evidence that a specific action or transaction has occurred. Non-repudiation services should be able to produce legally binding evidence. Non-repudiation services consist of the following services, non-repudiation of origin, non-repudiation of submission, and non-repudiation of delivery. Non-repudiation of origin protects against a message originator denying that a message was sent. Non-repudiation of submission protects against a Message Transfer Agent denying that a message was submitted for delivery. Non-repudiation of delivery protects against a message recipient denying that a message was received.

Non-repudiation is commonly implemented in financial systems where electronic funds transfers take place. An application developer utilizes the non-repudiation service through an application developer toolkit or third party services. For non-repudiation services to work, many legal aspects and issues must be resolved. This may be the biggest challenge. It is important to understand how non-repudiation is meant to be used and what the requirements are. The requirements may have to take both local and international laws into consideration, especially in the case of e-Commerce transactions which cross international borders.

SECURITY MANAGEMENT SERVICES

The operational aspects of any security solutions need to be considered alongside the security aspects. Security Management Services are services which intersect with both enterprise operations management and security management. Security Management Services tries to identify some of the interfaces which need to be in place. An example is an enterprise directory which may be administered by the Help Desk function, but which the Security Organization must develop and monitor. Security management services include, but are not limited to, enterprise and user management, policy management, certificate and key life-cycle management, availability and performance management, and directory integration and administration services.

ENTERPRISE/USER MANAGEMENT

Enterprise user management is commonly a central function in an enterprise provided by the Help Desk. Central user management is an important tool to administer all users across multiple systems and environments. Enterprise user management is a function provided as part of an operations architecture but with close ties to the security organization. The security organization may be a part of enterprise operations or alternatively be a completely separate organization.

Responsibilities should be clear as to who performs what functions between enterprise operations and the security organization. A role-based access control system should be considered. A role-based system is one with clearly defined responsibilities for each function and role. Once implemented, a role-based access control system is more flexible as an organization changes.

POLICY MANAGEMENT SERVICES

Between the enterprise operations management and the security organization there needs to be clear responsibilities for policies and how they are to be implemented, managed and enforced. A close working relationship is required. Areas that need to be addressed include, for example, backup/restore, file transfer, disaster recovery, event management, systems and network management. In each one of these areas there are security considerations and the policies should detail how these security considerations are being met.

CERTIFICATE/KEY SERVICES

As part of a Public Key Infrastructure, the life-cycle of certificates and keys must be managed. The options are to outsource to a third party the management of the PKI or to implement it and manage it internally. Certificate / Key life-cycle management services include Registration services, Distribution Services, Recovery Services, Storage Services and Revocation Services.

The management of certificates / keys throughout their life-cycle is a very important part of PKI. There may be legal requirements to follow as well as numerous technical and operational challenges. The management of the PKI is the most important aspect for its success.

AVAILABILITY AND PERFORMANCE SERVICES

Most security services and solutions have high availability and high performance requirements. This is due to the fact that the security services often are mission critical or are used by mission critical systems. The operational aspects of the security solutions need to be considered alongside the security aspects. When designing a security architecture which is mission critical, high availability and performance requirements need to be a part of that solution.

DIRECTORY INTEGRATION

If a directory server is being implemented it will most likely need to interface to other systems. If the directory contains user profiles which need to be managed the directory needs to be interfaced to the enterprise user management system. If the directory contains sensitive information, such as username/password and certificates, it must be kept secure.

CORE CAPABILITIES

The core capabilities of a security framework are the non-technology oriented portions, the areas of the framework that tend to be more people-oriented. These include security administration, security operations, security compliance, security development, security policy and standards, and security awareness. Other portions of the people aspect of security may include executive leadership, which is responsible for issuing security policy and providing resources to support a security function. The people aspect also may include department managers, responsible for communicating the value of security and staffing resources to meet standards which have been established through the security policy. End users are then responsible for complying with security policy, including protecting passwords, laptop

computers, their own desktop computers, and other forms of data or access to data and computer assets.

Security administration is concerned with administering safeguards, such as anti-virus software, and also administering user accounts, access rules, operating systems, firewalls, remote dial access, back ups, and the like. Back ups are typically remote storage sites that automatically receive and record computer information at intervals, such as every night, in case of disaster to the primary computer system.

Security operations investigate breaches of security, intrusions, fraud and errors in operations. Security compliance performs audits and reviews, performs risk assessment, performs intrusion detection and tests the security function for penetration and ease of penetration. Security development designs and develops secure applications, evaluates new security products, establishes security architectures, and researches new risks to the computer assets of an organization. Security policy and standards develops a security policy, develops standards to enforce the policy, and guidelines for operation of the computer security function. A security awareness function makes users alert to the need for personal security conduct and an awareness program, and also distributes alerts when computer security events occur or are imminent or threatened.

COMPUTER ASSETS AND KEY PROCESSES

The technology architecture and core capabilities protect the computer assets and key processes central to the business or enterprise. The key processes may include computer processes or manual processes dependent on computers or stored in a computer medium. Key process to be protected may also include security management, security strategy and risk management of an enterprise. Security strategy defines the approach and direction the company is taking to secure the assets. Security strategy sets the future directions for information security and affects all areas of security within a company. Its primary goal is to give an overview of the future business or enterprise directions and the security controls which should be in

place to support those functions. The security strategy determines the overall plan for the security based on new threats, user requirements, development requirements or vendor strategies. The security strategy must be aligned with other business or enterprise strategies to ensure that security is considered when new capabilities and acquisitions are planned, new alliances are made, and when new markets are entered. The strategies must work together.

Security management has overall responsibility for the management of the secure enterprise. Security management coordinates with other security areas, including the core capabilities mentioned above. Security management deals more with the people aspect of computer security, and an overview of how security will be managed, rather than the day-to-day functions performed by security features and security personnel. Security management initiates and manages enterprise-wide security programs to support the corporation's goals. Security management will develop, build and maintain the security organization and shape its structure. For example, decisions to decentralize security functions and to define the reporting structure belong to security management.

Risk management is also a high-level description of management's aversion to risk, and may include broad policies and procedures concerning the degree of assurance, or non-risk, implemented for computer operations. Risk management identifies the level of protection required and discovers the threats and vulnerabilities that must be addressed through the security strategy. Risk management handles the overall risks associated with a company or an enterprise. A security risk assessment is performed as part of the risk management function.

Another aspect of the invention is a method of designing and operating a security framework for a netcentric computer system. The method comprises the steps of performing a risk assessment, and then defining a security policy, determining appropriate computer security controls, and implementing the policy and the controls. Operating the system and the framework will then include managing the security framework and the controls, in light of the announced and implemented security policy. At

certain times, it may be appropriate to review the security policy, the controls, and the compliance thereto. One portion of operating such a system is to respond to any security events, such as a security threat, a breach, or other risks to computer assets.

It will be appreciated that a wide range of changes and modifications to the method as described are contemplated. Accordingly, while preferred embodiments have been shown and described in detail by way of examples, further modifications and embodiments are possible without departing from the scope of the invention as defined by the examples set forth. It is therefore intended that the invention be defined by the appended claims and all legal equivalents.

While this invention has been shown and described in connection with the embodiments described, it is apparent that certain changes and modifications, in addition to those mentioned above may be made from the basic features of this invention. Many types of organizations may benefit from the use of this invention, e.g., any organization wishing to use a security system or security framework in cooperation with a computer system or an information technology system. These are not limited to commercial businesses, and may include governmental organizations and non-governmental organizations, such as charitable, civic, educational, cultural or other non-profit groups. In addition, there are many different types of computer systems, and computer software and hardware that may be utilized in practicing the invention, and the invention is not limited to the examples given above. Accordingly, it is the intention of the applicants to protect all variations and modifications within the scope of the present invention. It is intended that the invention be defined by the following claims, including all equivalents.

We Claim:

1. A security architecture framework for a netcentric computer system, comprising:

a computer network;

a server connected with the network;

a client connected with the network; and

a computer security system protecting the network, the server and the client, wherein the computer security system comprises a security infrastructure, and security services.

2. The framework of Claim 1, wherein said security infrastructure comprises core security components and security tools.

3. The framework of Claim 2, wherein said security components include at least one of registration and identification, authentication, single sign-on, access control, encryption, digital notarization, content and virus inspection, logging, non-repudiation, firewall, public key infrastructure, platform security, and virtual private networks.

4. The framework of Claim 3, wherein registration and identification includes at least one of ensuring proper identification, verifying data, authorizing registration, and checking a directory or meta-directory.

5. The framework of Claim 4, where proper identification is assured by verifying at least two data during registration.

6. The framework of Claim 3, wherein authentication is accomplished by a username and password, and wherein the username and password are encrypted when transferring the password.

7. The framework of Claim 3, wherein authentication is accomplished by a username and password, certificates, time-dependent passwords, and biometrics.

8. The framework of Claim 3, wherein an access control product includes at least one of a firewall, a security operating system, a security network operating system, a specific access control product, Web access control, and role-base access control.

9. The framework of Claim 3, wherein enterprise assets are protected by a firewall, and access is restricted to authorized users.

10. The framework of Claim 3, wherein data is encrypted before transmission.

11. The framework of Claim 3, wherein incoming data is inspected for content and viruses before admission to the netcentric computer system.

12. The framework of Claim 3, wherein the security components include a check that platforms, servers, and interconnections between platforms and servers are free from intrusion.

13. The framework of Claim 2, wherein said security tools include at least one of intrusion detection and vulnerability assessment.

14. The framework of Claim 1, where said security services comprise security base services and security management services.

15. The framework of Claim 3, wherein registration and identification further include at least one of on-line registration, data verification services, a registration authority, a directory and a meta-directory.

16. The framework of Claim 3, wherein authentication is by at least one of username and password, token and one-time password, a certificate, a time-dependent password, a biometric method, a smartcard, an authentication server, a directory, and a public key infrastructure.

17. The framework of Claim 3, wherein single sign-on is by at least one of cookies and session management, an access control product, a scripting solution, and password synchronization.

18. The framework of Claim 3, wherein access control is by at least one of a firewall, an operating system, a network operating system, an access control product, web access control, and role-based access control.

19. The framework of Claim 14, wherein said security base services include at least one of registration and identification services, authentication services, single sign-on services, access control services, encryption services, digital notarization services, content and virus inspection services, logging services, and non-repudiation services.

20. The framework of Claim 14, wherein said security management services include at least one of enterprise user management services, policy management services, certificate or key life-cycle management services, availability and performance services, and directory integration and administration services.

21. The framework of Claim 1, further comprising at least one computer asset, at least one key process, and core capabilities to protect the at least one computer asset and the at least one key process.

22. The framework of Claim 21, wherein the core capabilities include at least one of security administration, security operations, security compliance, security development, security policy and standards, and security awareness.

23. The framework of Claim 21, wherein the at least one key process includes at least one of security management, security strategy, and risk management.

24. The framework of Claim 21, wherein the at least one computer asset includes at least one of a computer file, a tape, a disc, a storage medium, a software program, an application, a computer, a system and a network.

25. The framework of Claim 22, wherein security administration includes administering at least one of anti-virus software, user accounts, access rules, operating systems, firewalls, remoter dial access, and backups.

26. The framework of Claim 22, wherein security operations includes investigating at least one of breaches, intrusions, errors and fraud.

27. The framework of Claim 22, wherein security compliance includes at least one of performing audits and reviews, performing intrusion and detection, performing risk assessment, and testing penetration.

28. The framework of Claim 22, wherein security development includes at least one of designing a secure application, developing a secure application, evaluating a security product, establishing a security architecture, and researching a new risk.

29. The framework of Claim 22, wherein security policy and standards includes developing at least one of a security policy, a security standard, and a security guideline.

30. The framework of Claim 22, wherein security awareness includes at least one of distributing an alert, developing an awareness program, and delivering an awareness program.

31. A method of operating a netcentric security framework in a computing system, comprising:

providing a security infrastructure for the system;

providing security services for the system;

developing security procedures and processes for the system;

maintaining security policy and standards for the system;

conducting secure operations within the computing system; and

making users aware of the need for computer security,

to protect computer assets of an enterprise.

32. The method of Claim 31, wherein the security infrastructure comprises core security components and security tools.

33. The method of Claim 32, wherein the security components further comprise at least one of registration and identification, authentication, single sign-on, access control, encryption, digital notarization, content and virus inspection, logging, and non-repudiation.

34. The method of Claim 32, wherein the security tools further comprise at least one of intrusion detection and vulnerability assessment.

35. The method of Claim 31, wherein the security services comprise security base services and security management services.

36. The method of Claim 35, wherein the security base services further comprise at least one of registration and identification services, authentication services, single sign-on services, access control services, encryption services, digital notarization services, content and virus inspection services, logging services, and non-repudiation services.

37. The method of Claim 35, wherein the security management services further comprise at least one of enterprise user management services, policy management services, certificate or key life-cycle management services, availability and performance services, and directory integration and administration services.

38. The method of Claim 33, where registration and identification include at least one of on-line registration, data verification services, a registration authority, a directory, and a meta-directory.

39. The method of Claim 38, wherein authentication is by at least one of username and password, token and one-time password, a certificate, a time-dependent password, a biometric method, a smartcard, an authentication server, a directory, and a public key infrastructure.

40. The method of Claim 38, wherein single sign-on is by at least one of cookies and session management, an access control product, a scripting solution, and password synchronization.

41. The method of Claim 38, wherein access control is by at least one of a firewall, an operating system, a network operating system, an access control product, web access control, and role-based access control.

42. A method for designing a netcentric security framework in a computing system for an organization, comprising:

providing a security infrastructure for the system, said security infrastructure comprising technical and non-technical components of a security framework;

providing security services for the system;

providing security functions for the system; and

providing security process to support the security infrastructure and services,

wherein computer assets of the organization are protected by the security framework.

43. The method of Claim 42, further comprising:

providing security procedures and processes;

providing a security policy and security standards;

providing security operations to administer the security framework; and

providing security awareness for a user of the computer system, to develop and maintain the netcentric security framework.

44. A method of auditing a netcentric security framework technical architecture, comprising:

reviewing security components in a security infrastructure and testing security services in a security framework.

45. The method of Claim 44, wherein the security components include at least one registration and identification, authentication, single sign-on, access control, encryption, digital notarization, content and virus inspection, platform security, and virtual private networks.

46. The method of Claim 45, where the step of checking authentication includes a check of the ease of guessing a password or brute-force discovery of the password.

47. The method of Claim 44, wherein the security services include at least one of security base services and security management services.

48. The method of Claim 47, wherein the step of testing security management services includes testing at least one of enterprise/user management, policy management, certificate/key services, availability and performance services, and directory integration and administration.

49. The method of Claim 47, wherein the step of testing includes testing enterprise/user management for compliance with security policy.

50. The method of Claim 47, wherein the step of testing includes testing for intrusion detection and vulnerability assessment.

51. A method of designing and operating a security framework for a netcentric computer system, comprising:

performing a risk assessment;

defining a security policy;

determining security controls in light of the risk assessment;

implementing the policy and the controls;

managing the controls;

reviewing the controls; and

responding to a security event,

wherein a security event is a violation of the controls.

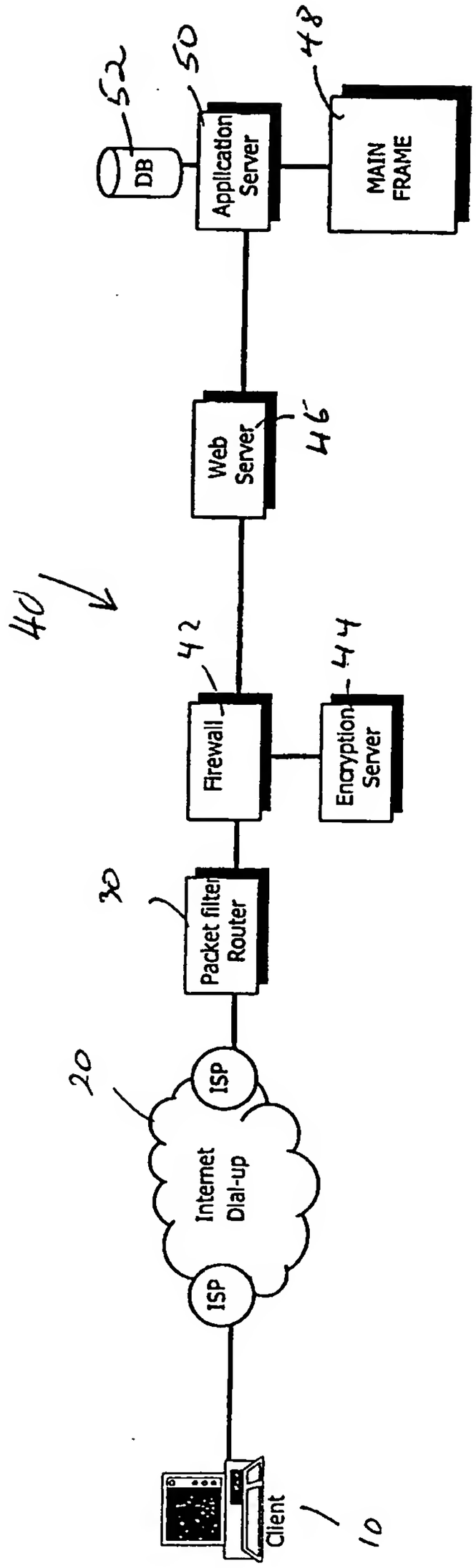


FIG. 1

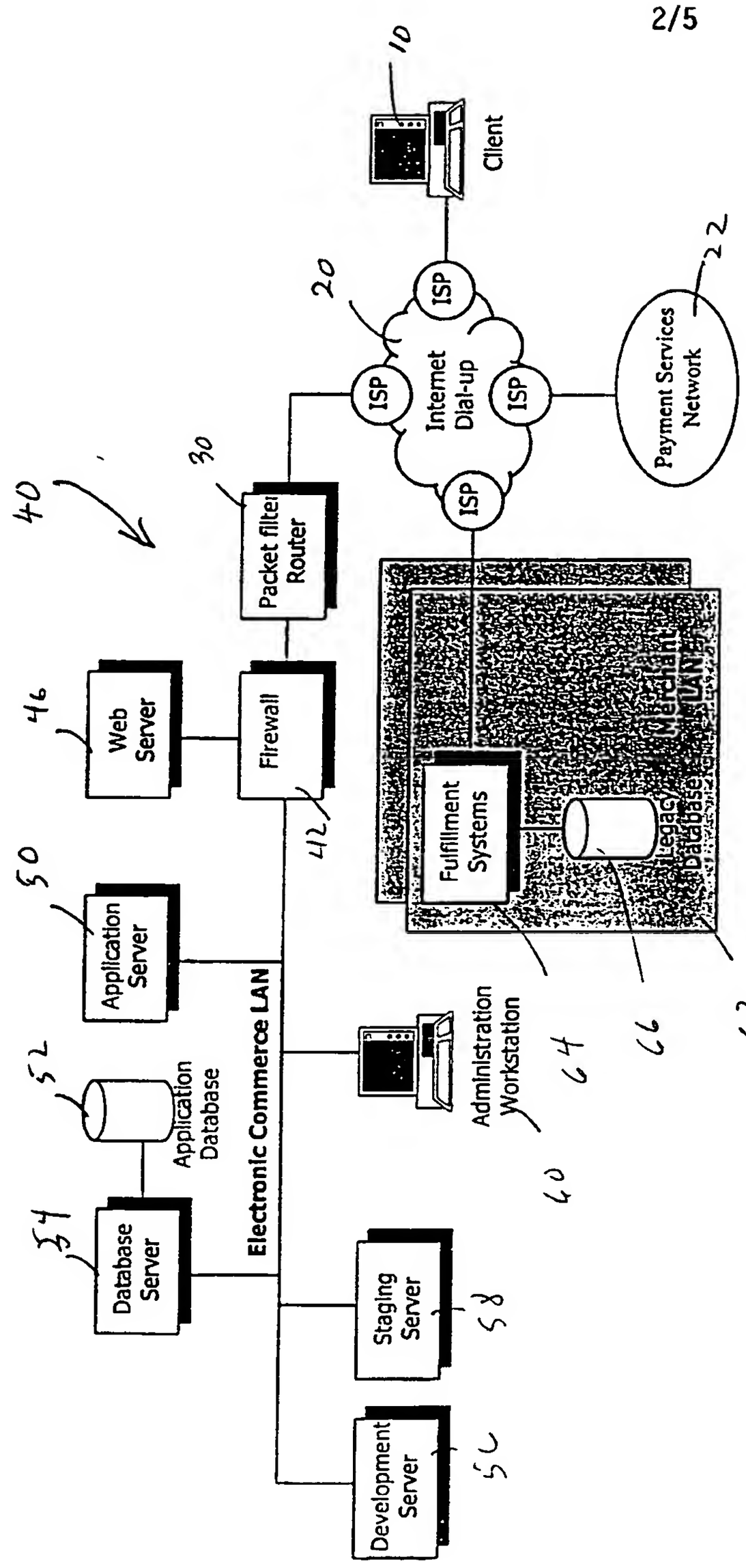


FIG 2

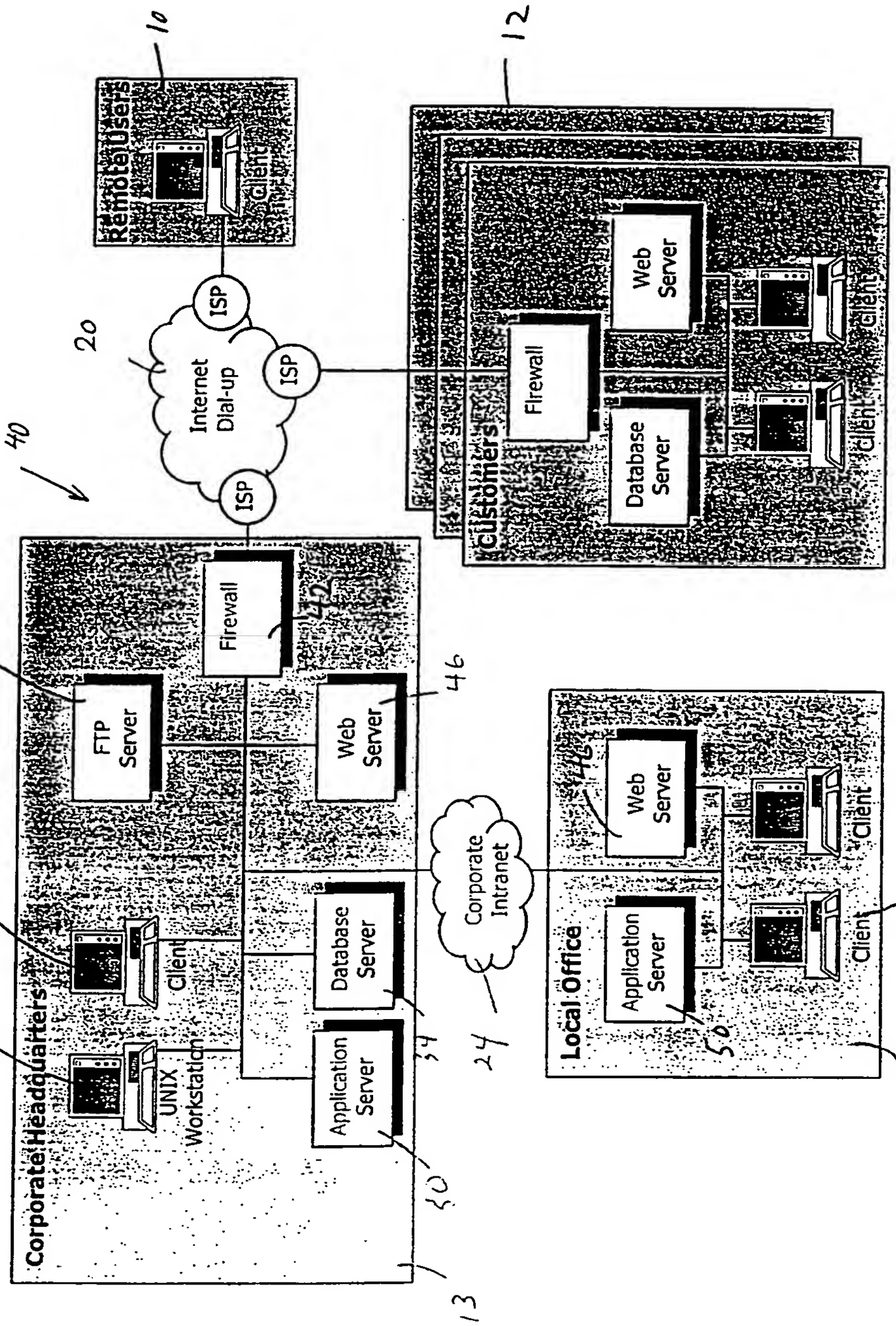


Fig 3.

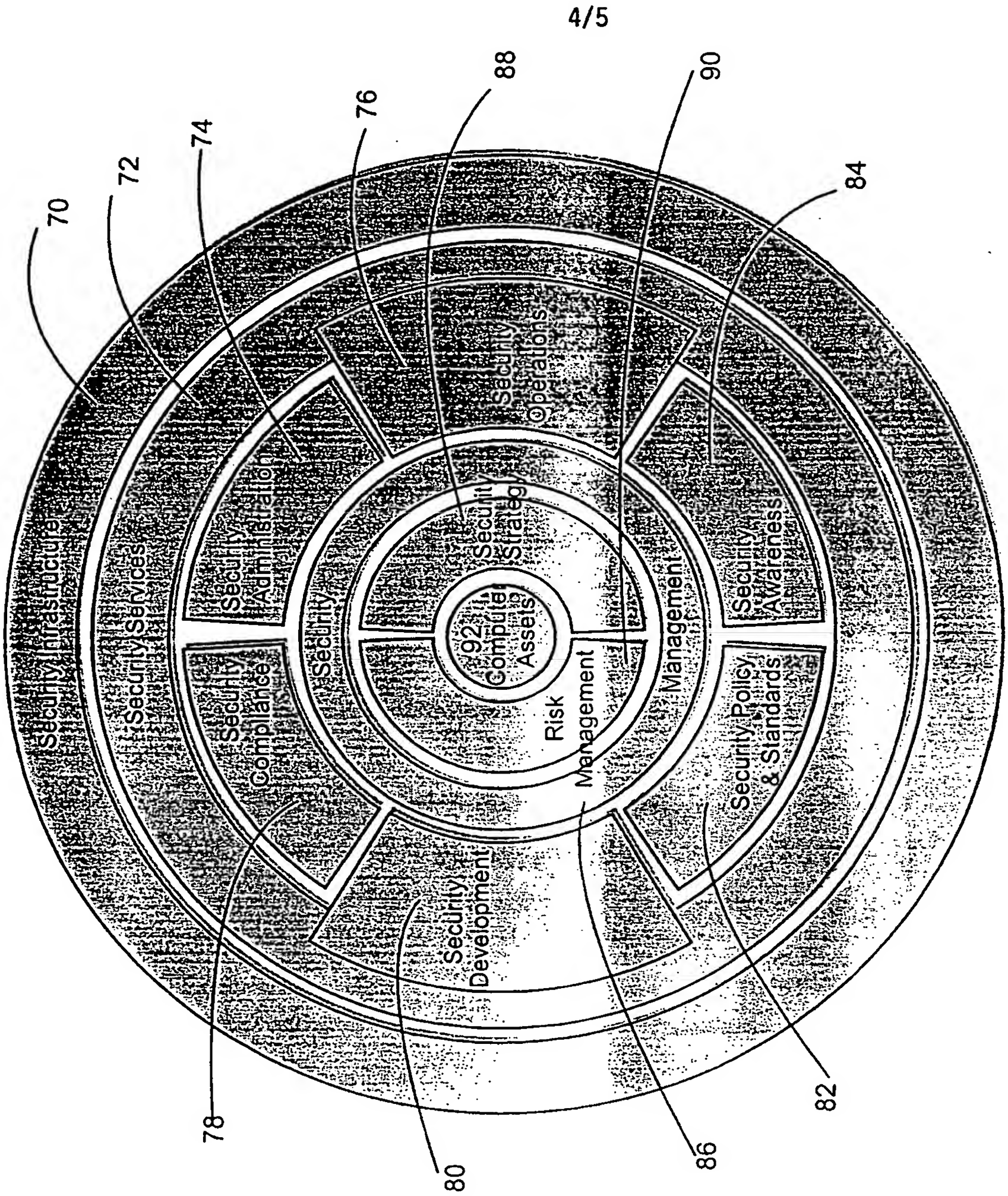


Fig. 4

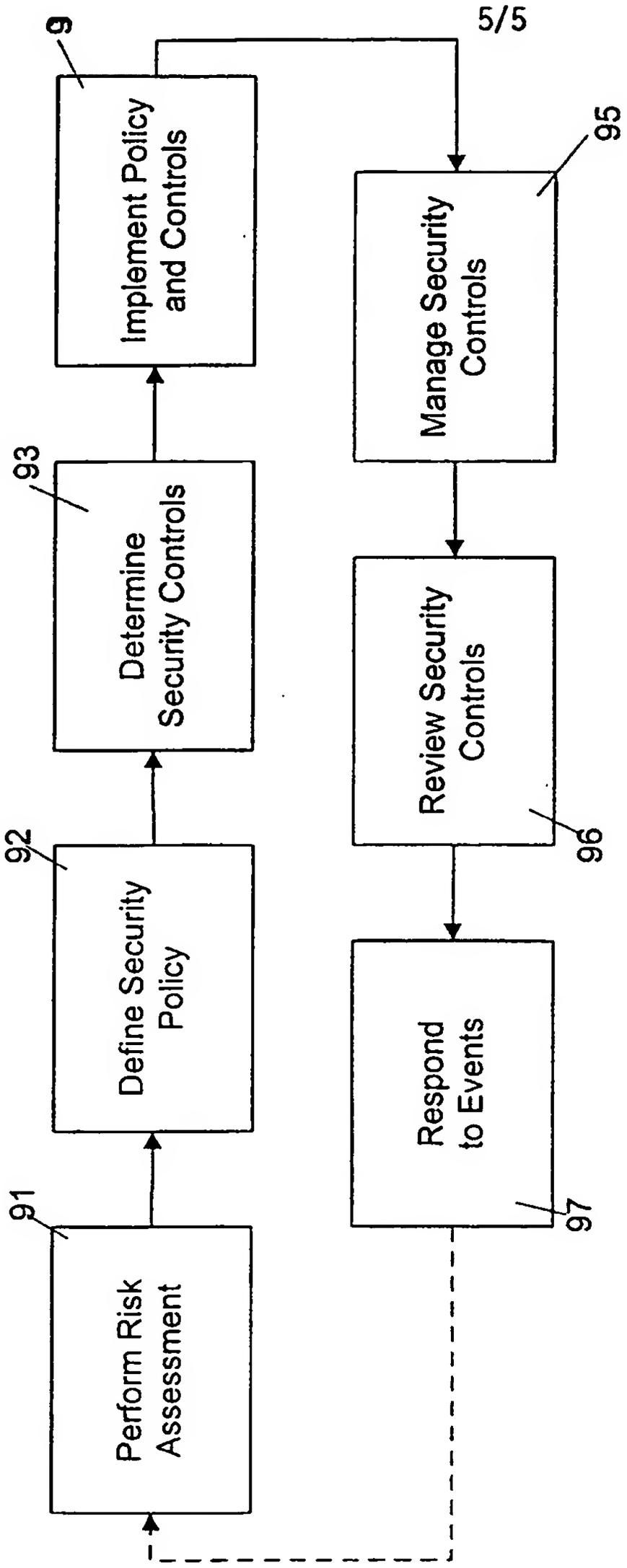


Fig. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/30420

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G06F 11/30; H04L 9/00
US CL : 713/ 200-202, 156-157, 168-171, 173, 183
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 713/ 200-202, 156-157, 168-171, 173, 183

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

NONE

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EAST, USPAT, IBM TBD, JAPIO; terms searched: authentication, security, authenticate, validation, secure, remote, auditing, detect?, vira?.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,923,756 A (SHAMBROOM) 13 July 1999, see entire document.	1-51
Y	US 5,748,890 A (GOLDBERG et al.) 05 May 1998, see entire document.	1-51.
Y	US 5,560,008 A (JOHNSON et al.) 24 September 1996, see entire document.	1-51
Y,P	US 6,092,196 A (REICHE) 18 July 2000, see entire document.	1-51
Y,P	US 6,076,168 A (FIVEASH et al.) 13 June 2000, see abs.	1, 31,42,51
Y,E	US 6,182,229 B1 1 (NIELSEN) 30 January 2001, see entire document.	1-51.

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search	Date of mailing of the international search report
26 FEBRUARY 2001	02 APR 2001
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer James R. Matthews NORMAN MICHAEL WRIGHT Telephone No. (703) 308-0000

Form PCT/ISA/210 (second sheet) (July 1998)★